ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ТУЛЬСКОЙ ОБЛАСТИ «ТУЛЬСКАЯ ШКОЛА»
(ГОУ ТО «ТУЛЬСКАЯ ШКОЛА»)

Приложение № 1 к приказу
от 30.08.2024 № 79-осн

ПРИНЯТО на заседании
общего собрания работников
ГОУ ТО «Тульская школа»
протокол от 26.08.2024 № 1

УТВЕРЖДЕНО
приказом ГОУ ТО «Тульская школа»
от 30.08.2024 № 79-осн

ПОЛИТИКА АНТИВИРУСНОЙ ЗАЩИТЫ В ГОУ ТО «ТУЛЬСКАЯ ШКОЛА»

г. Тула

1. Термины и определения

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Антивирусная защита (АВЗ)- набор средств и методов, направленных на борьбу с угрозами компьютерных вирусов (вредоносного программного обеспечения).

Вредоносное программное обеспечение (вредоносное ПО)

- любое программное обеспечение, предназначенное для получения несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы (автоматизированной системы).

Компьютерный вирус (вирус) - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (закон РФ от 21 июля 1993 г. № 5485 «О государственной тайне»).

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (закон РФ № 149-ФЗ);

Государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов (закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»);

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Обращение гражданина - направленные в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба;

Корпоративная электронная почта - система электронной почты, принадлежащая ОГВ Тульской области, используется сотрудниками только для выполнения ими служебных заданий. ОГВ оплачивает почтовый трафик, а также рабочее время, потраченное сотрудниками на обработку электронной почты. Он же несет убытки в случае утечки конфиденциальной информации.

Нежелательная почта (спам) - телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя.

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

Фишинг - вид интернет-мошенничества, цель которого является получение идентификационных данных пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Антивирусное программное обеспечение (антивирусное ПО, средство антивирусной защиты) — любая программа для обнаружения компьютерных вирусов, нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Машинный носитель информации (МНИ) - любое техническое устройство, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации (магнитный, лазерный, USB - носитель).

Средство вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

2. Назначение и область действия

2.1. Политика антивирусной защиты информации определяет основные правила и требования по защите информационных ресурсов от угроз, связанных с воздействием программ, специально разработанных или модифицированных для несанкционированного уничтожения, блокирования, модификации, копирования информации, а также нарушения нормального функционирования элементов АС.

2.2. Настоящая Политика разработана в соответствии с следующими нормативно правовыми актами в области информационной безопасности:

- приказом ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,
- приказом ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- федеральным законом Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
- федеральным законом Российской Федерации от 2 мая 2006 г. N 59- ФЗ "О порядке рассмотрения обращений граждан Российской Федерации";

2.3. Политика АВЗ определяет основные принципы построения и использования в ОГВ системы антивирусной защиты на основе антивирусного ПО и системы фильтрации входящего почтового траффика в домене tularegion.ru и tularegion.org (системы защиты пользователей корпоративной почты ОГВ) с распределением зон ответственности.

2.4. Политика распространяется на государственных гражданских служащих и работников органов исполнительной власти Тульской области, аппарата

правительства Тульской области, работников подведомственных им учреждений, а также третьих лиц, использующими информационные ресурсы локальной вычислительной сети правительства Тульской области (далее - пользователь), и является обязательной для исполнения.

2.5. Для органов местного самоуправления Тульской области и подведомственных им учреждений настоящий документ носит рекомендательный характер.

3. Основные типы вирусных угроз информационной безопасности

3.1. Компьютерные вирусы остаются в настоящее время одной из наиболее опасных угроз информационной безопасности в АС. Главными видами угроз антивирусной безопасности являются различные типы вредоносного ПО, способного нанести ущерб АС или её пользователям.

3.2. Основным условием вирусной угрозы в АС является наличие уязвимости, на основе которой потенциально возможно провести вирусные атаки. Уязвимости могут возникать из-за недостатков организационно-правового либо программно-аппаратного обеспечения АС.

3.3. Уязвимости организационно-правового обеспечения обусловлены отсутствием или нарушением требований нормативных и организационно-распорядительных документов, в которых определяются требования к антивирусной безопасности в АС.

3.4. Уязвимостями программно-аппаратного обеспечения являются: ошибки в программном обеспечении; отсутствие средств защиты информации; неправильная конфигурация программного обеспечения; использование простых и нестойких паролей и другие факторы. Уязвимости могут возникать как на технологическом, так и на эксплуатационном уровне АС. Технологические уязвимости проявляются на стадиях проектирования, разработки и развёртывания АС. Эксплуатационные уязвимости связаны с неправильной настройкой программно-аппаратного обеспечения, установленного в АС.

3.5. Электронная почта является одним из основных каналов проникновения в информационную систему ОГВ Тульской области вредоносного ПО, сообщений рекламного или мошеннического характера. Доступность системы электронной почты дает возможности пользователям применять систему для рассылки спама.

4. Порядок обработки, передачи и приема документов по электронной почте

4.1. Секретарь руководителя обеспечивает бесперебойное функционирование электронной почты[1] в течение всего рабочего времени.

4.2. При получении важных писем, требующих подтверждения ответа, секретарь руководителя обязана отправить такое подтверждение. Секретарь руководителя должна принять все, зависящие от нее, меры для обеспечения правильной настройки почтового клиента для возможности отправки подтверждения получения писем в штатном режиме.

---

[1] Под бесперебойным функционированием электронной почты подразумевается работа почтового клиента с включенным звуковым и визуальным оповещением получения электронных писем в течение всего рабочего дня. Подтверждение получения (если необходимо) должно отправляться сразу после получения сообщения.

4.3. Перед отправлением сообщения необходимо проверять правописание и грамматику текста сообщения. Тексты большого объема желательно отправлять в виде вложения.

4.4. При получении «спама» (нежелательные электронные письма, как правило, рекламного характера), секретарь руководителя обязан сразу удалить такие письма, не открывая вложение (желательно добавить отправителя в список заблокированных отправителей).

4.5. Передаваемые с помощью электронной почты официальные документы должны иметь соответствующие реквизиты (исходящий регистрационный номер, номер и дату приказа, распоряжения и т.п.). В тексте сообщения необходимо обязательно указывать реквизиты и название пересылаемого во вложении официального документа. Передаваемая и принимаемая в адрес Учреждения официальная электронная корреспонденция регистрируется в соответствии с правилами делопроизводства, установленными в Учреждении.

4.6. При получении электронного сообщения секретарь руководителя регистрирует его в установленном порядке и передает на рассмотрение руководителю Учреждения.

4.7. В случае невозможности прочтения электронного сообщения, секретарь руководителя уведомляет об этом отправителя.

5. Классификация вредоносного ПО (вирусов)

5.1. Все вредоносное ПО можно классифицировать по следующим основным признакам:

а) по воздействию на СВТ и информацию;

б) по типу вредоносного ПО (особенностям алгоритма);

в) по способу заражения (проникновения в СВТ);

г) по объекту, на который направлено воздействие.

5.2. Воздействие на СВТ и информацию.

а) Очень опасные вирусы. Эти вирусы могут уничтожить определенные или все данные, находящиеся на МНИ СВТ, изменить настройки операционной системы или полностью вывести ее из строя и т.д.

б) Опасные вирусы. Могут привести к сбоям в работе операционной системы СВТ или программного обеспечения установленного на СВТ.

в) Неопасные вирусы. Данные вирусы не мешают работе СВТ, но могут уменьшать объем свободной оперативной памяти, памяти на МНИ. Действие таких вирусов проявляется в каких-либо графических или звуковых эффектах.

5.3. Тип вредоносного ПО (особенности алгоритма).

5.3.1. ***Компьютерный вирус и компьютерный червь*** — это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь может не подозревать о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

5.3.2. ***Троянские программы*** — это вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать: удаление данных; блокирование данных; изменение данных; копирование данных;

несанкционированная загрузка другого вредоносного программного обеспечения; замедление работы СВТ и компьютерных сетей. В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению.

5.3.3. Троянские программы классифицируются в соответствии с типом действий, выполняемых ими на СВТ.

Бэкдоры. Троянская программа бэкдор предоставляет злоумышленникам возможность удаленного управления зараженным СВТ. Такие программы позволяют злоумышленнику выполнять на СВТ любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку СВТ. Троянцы-бэкдоры часто используются для объединения группы компьютеров-жертв в ботнет или зомби-сеть для использования в криминальных целях.

Эксплойты. Это вредоносные программы использующие уязвимости в установленном на СВТ программном обеспечении.

Руткиты. Это вредоносные программы, предназначенные для сокрытия в системе определенных объектов или действий. Часто основная их цель — предотвратить обнаружение вредоносных программ, чтобы увеличить время работы этих программ на зараженном СВТ.

Шпионские программы. Программы данного типа способны скрыто наблюдать за использованием СВТ, например, отслеживая вводимые с клавиатуры данные, делая снимки экрана и получая список работающих приложений.

И многие другие виды троянских программ.

5.4. Способ заражения (проникновения в СВТ, АС).

5.4.1. Вирусы проникают в СВТ и АС посредством локального или сетевого взаимодействия.

5.4.2. Локальное взаимодействие предполагает использование съемных носителей, таких как диски CD-ROM или DVD-ROM, USB- накопители, а также карты дополнительной памяти. Инфицирование АС в этом случае осуществляется при запуске зараженного файла.

5.4.3. Для инфицирования АС через сетевое взаимодействие используется один из следующих каналов:

- электронная почта (входящие электронные письма, содержащие вложения с вредоносным ПО или ссылки на вредоносное ПО);
- сетевые каталоги и файлы (вероятность скачивания, загрузки вредоносного ПО);
- системы обмена мгновенными сообщениями (Mail-агент, Skype, ICQ- агент и т.д.);
- ресурсы сети Интернет (сайты).

5.5. Объект, на который направлено воздействие.

5.5.1. Вирусы могут воздействовать на аппаратное, общесистемное или прикладное программное обеспечение, а также на информацию, которая обрабатывается в АС. Воздействие вирусов на аппаратное обеспечение, как правило, направлено на несанкционированное изменение памяти микросхемы BIOS. В результате может быть искажено ее содержимое, что приведет к блокированию возможности загрузки СВТ.

5.5.2. При воздействии на общесистемное и прикладное ПО вирусы модифицируют компоненты операционных систем, а также программ, которые на ней установлены. Для ликвидации последствий необходимо восстановление

отдельных файлов или переустановка инфицированных программ.

5.5.3. Воздействие на информационном уровне направлено на объекты данных, которые обрабатываются общесистемным и прикладным программным обеспечением АС. Примерами объектов являются - файлы, таблицы баз данных, хранилища электронной почты, адресные книги пользователей и др.

5.6. К основным угрозам, возникающим при обработке корпоративной электронной почты, относятся:

***Вредоносное** ПО* любых разновидностей, перечисленное в п. 4.3;

Целевой и нецелевой спам. Как правило, это письма, содержащие навязчивые предложения самых разнообразных услуг, товаров и т.п. Такого рода почта является "группой риска" с точки зрения переноса вирусов. Большое количество ненужной почты загружает каналы, "замусоривает" почтовые ящики, отнимает время на удаление ненужных писем и повышает вероятность случайного удаления нужных;

Утечка конфиденциальной информации - организуется с использованием тех или иных мошеннических схем. Одним из наиболее частых способов является выдача мошенником своего письма за письмо от сторонней, доверенной для адресата, организации;

Отказ в обслуживании - возможное целенаправленное выведение почтового сервера адресата, например в результате переполнения поступающими сообщениями.

6. Политика использования Интернет

6.1. Использование сети Интернет в Учреждении осуществляется, в целях образовательного процесса.

6.2. Учреждение не несет ответственности в случае возникновения последствий опубликования персональных данных, если имелось письменное согласие лица (его представителя) на опубликование персональных данных.

6.3. Работающим в сети Интернет, запрещается:

- размещать собственную информацию в Интернет на Интернет-ресурсах Учреждения;
- иметь учетную запись электронной почты на Интернет-ресурсах Учреждения;
- находиться на ресурсах, содержание и тематика которых является недопустимой и/или нарушающей законодательство Российской Федерации (порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

7. Основные принципы антивирусной защиты

7.1. Антивирусная защита строится на основе следующих основных принципов:

Комплексность. Обеспечение антивирусного контроля всех информационных потоков, проходящих как внутри АС, так и выходящих за ее пределы.

Эшелонированность. Проверка информационных потоков на нескольких уровнях: при входе в информационную систему, при обработке, передаче и хранении информации внутри информационной системы.

Совмещение. Использование средств разных ведущих производителей для повышения вероятности обнаружения вредоносного программного обеспечения и вирусов на разных уровнях.

Управляемость. Осуществление централизованного контроля наличия, работоспособности антивирусных средств, оперативной информации об обнаружении вирусов и других вредоносных программ, централизованного обновления антивирусных баз и т.д. подразделениями (должностными лицами), ответственными за антивирусную защиту.

Ответственность. Определение персональной ответственности должностных лиц за мероприятия по АВЗ, закреплённые в должностных регламентах, положениях, инструкциях.

7.2. К принципам АВЗ также относится:

а) использование в работе на СВТ только лицензионного программного обеспечения;

б) периодическое создание архивных (резервных) копий файлов, с которыми ведётся работа, в соответствии с дополнительными инструкциями;

в) проверка всех МНИ, полученных от сторонних организаций и граждан, на наличие вирусов перед их использованием;

г) проверка всего почтового трафика и интернет-трафика на наличие вирусов в автоматическом режиме.

д) периодическая проверка СВТ на наличие вирусов с использованием актуальной версии антивирусной программы и актуальными базами вирусных сигнатур;

е) использование антивирусного ПО, соответствующего применяемому в конкретном случае программному обеспечению и имеющего сертификаты соответствия Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

ж) своевременное обновление операционных систем и прикладных программ, предназначенное для устранения уязвимостей в их безопасности.

з) все электронные сообщения, поступающие на корпоративные почтовые ящики сотрудников ОГВ подвергаются фильтрации для удаления нежелательной почты, фишинговых сообщений, вредоносных ссылок и вложений, за исключением специально созданных почтовых ящиков ОГВ для получения обращений граждан.

и) очистка почтового траффика осуществляется специализированным ПО, установленным и функционирующим на внешних почтовых транспортных серверах почтовой системы tularegion.ru и tularegion.org. Тем самым блокировка нежелательной почты осуществляется перед попаданием корреспонденции от внешних почтовых сервисов в защищенный периметр ОГВ Тульской области.

7.3. Объектами антивирусной защиты являются:

а) серверы в локальных вычислительных сетях (ЛВС);

б) АРМ в ЛВС и вне их;

в) прикладные программы и их базы данных;

г) портативные АРМ (ноутбуки);

д) мобильные, переносные и другие личные устройства пользователей, с

которых осуществляется доступ к ресурсам АС.

е) абонентские ящики корпоративной почты сотрудников защищаемых организаций.

8. Построение антивирусной защиты

8.1. На всех рабочих станциях и серверах органов исполнительной власти Тульской области, подразделений аппарата правительства Тульской области и подведомственных учреждениях Тульской области (далее - ОГВ), если иное не предусмотрено технологическим процессом, в обязательном порядке должны применяться средства антивирусной защиты.

8.2. Процедуры установки и регулярного обновления средств антивирусной защиты (версий антивирусных баз) на СВТ ОГВ должны быть документированы и осуществляться администраторами антивирусной защиты или уполномоченными лицами. Необходимо использовать автоматический режим установки обновлений баз антивирусных сигнатур. Обновление версий антивирусного ПО в ОГВ должно производиться только по решению руководителя органа по информационной безопасности ГАУ ТО «ЦИТ», администратором антивирусной защиты информации с привлечением службы поддержки пользователей ГАУ ТО «ЦИТ».

8.3. Обеспечение актуальности баз данных (сигнатур) антивирусных программных средств производится периодическим их обновлением (пополнением). Первичным источником обновления являются специализированные Интернет-ресурсы - сайты производителей антивирусных средств, вторичным - специальные внутренние сетевые ресурсы или МНИ. Вторичные источники обновляются из первичных.

8.4. Вторичные источники обновления организуются для минимизации необходимости доступа к ресурсам Интернет и используются для обновления антивирусного программного обеспечения внутри ЛВС. Периодичность обновления вторичных источников определяется периодичностью обновления первичных источников и практической необходимостью, но не реже одного раза в день.

8.5. В ОГВ организовывается функционирование постоянной антивирусной защиты в автоматическом режиме.

8.6. Должна обеспечиваться антивирусная фильтрация всего трафика электронного почтового обмена и интернет-трафика ОГВ.

8.7. Антивирусная защита строится по типу эшелонированной централизованной системы, предусматривающей возможное использование антивирусных средств различных производителей и обеспечивающее их раздельную установку на рабочих станциях, серверах, почтовых серверах и интернет-шлюзах.

8.8. В ОГВ применяются антивирусные средства, обеспечивающие защиту вне зависимости от действий пользователя объекта защиты, исключающие возможность изменения пользователем параметров настройки антивирусных программ.

8.9. Настройка антивирусного ПО Dr. Web выполняется в соответствии с Регламентом действий администратора антивирусной защиты по настройке антивирусного программного комплекса «Dr.Web Enterprise Security Suite» (Приложение № 1).

8.10. Настройка антивирусного ПО Лаборатории Касперского выполняется в

соответствии с Регламентом действий администратора антивирусной защиты по настройке антивирусного программного комплекса «Kaspersky Endpoint Security» (Приложение № 2).

8.11. В обязательном порядке выполняются процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. Результаты установки, изменения программного обеспечения и антивирусной проверки должны документироваться в программных журналах.

8.12. Все поступающие в ОГВ из сторонних организаций МНИ подвергаются проверке на наличие вирусов. При обнаружении на носителе зараженного и не поддающегося лечению файла дальнейшее использование носителя не допускается.

8.13. Адреса электронной почты, используемые ОГВ в качестве официальных почтовых ящиков для получения обращений граждан, добавляются в белый список получателей в настройках системы фильтрации входящей электронной почты домена tularegion.ru. Это необходимо для беспрепятственной доставки обращений граждан в ОГВ. Электронная почта, поступающая на эти адреса, проверяется только антивирусным модулем системы фильтрации входящего траффика почтового сервера. Перечень данных адресов представлен в приложении (Приложение № 3)

8.14. Установка и настройка компонентов системы защиты пользователей корпоративной почты (далее - СЗПКП) выполняется в соответствии с Регламентом действий администратора системы защиты корпоративной почты по настройке программы Kaspesky Security для Microsoft Exchange Servers (Приложение № 4).

9. Порядок реагирования на инциденты вирусного заражения СВТ

9.1. В случае выявления заражения СВТ (выявление признаков заражения) вредоносным ПО необходимо:

а) Пользователю ОГВ выключить АРМ имеющее признаки заражения (отключение электропитания от ПК) и незамедлительно сообщить о вирусном заражении в Службу поддержки пользователей телефону (4872) 25-32-16 и администратору безопасности ОГВ.

б) Информация, сообщаемая в Службу поддержки пользователей должна содержать данные:

- о времени обнаружения вредоносной программы;
- о принадлежности и назначении зараженного вычислительного средства;
- о признаках проявления деятельности вредоносной программы и (при наличии) классификации ее антивирусными средствами.

9.2. Служба поддержки пользователя ГАУ ТО «ЦИТ» информирует администратора антивирусной защиты и администратора безопасности ОГВ о факте заражения, проводит лечение, вредоносного ПО и выявление источника заражение, штатными средствами или с загрузочного антивирусного диска. Выполняется детальная оценка нанесенного урона хранимой на АРМ информации.

9.3. Администратором антивирусной защиты при отсутствии детектирования вредоносной программы штатными антивирусными средствами, подозреваемые в заражении файлы представляются производителям соответствующих средств антивирусной защиты. **Не допускается передача файлов с информацией ограниченного доступа.**

9.4. Администратором антивирусной защиты проводится анализ проникновения на СВТ вредоносного ПО и возможный ущерб ЛВС.

9.5. При выявлении источника и/или пути заражения, администратор антивирусной защиты оценивает вероятность распространения заражения на другие СВТ и запрашивает у администраторов специализированных систем информацию о возможных получателях вирусов, почтовых отправлениях с вредоносным ПО, файлах с типовым расширением и т.д. Администраторы специализированных систем предоставляют указанную информацию в кратчайшие сроки.

9.6. При выявлении признаков модификации информации осуществляемой вредоносным ПО на ресурсах общего доступа, администратор антивирусной защиты вправе отключить (дать запрос на отключение) данных ресурсов до момента выявления источника модификации информации. Служба поддержки пользователя информирует пользователей ОГВ о недоступности ресурсов общего доступа.

9.7. Руководителем ОГВ или министерством по информатизации, связи и вопросам открытого управления Тульской области выносится решение о необходимости обращения в правоохранительные органы в связи с инцидентом вирусного заражения (в случае возможности материальной оценки нанесенного ущерба).

10. Порядок действий по восстановлению исходного состояния средств вычислительной техники после вирусного воздействия

10.1. При обнаружении вирусного воздействия восстановление работоспособного состояния средств вычислительной техники производится:

а) администратором приложения, функционирующего на сервере, при поддержке администратора антивирусной защиты - в случае заражения сервера;

б) специалистом службы поддержки пользователей, при поддержке администратора антивирусной защиты - в случае заражения АРМ.

10.2. Восстановление исходного состояния ЛВС может производиться различными способами, но с соблюдением обязательных правил:

а) зараженные СВТ отключить от сети, прекратить также (при необходимости) взаимодействие с другими ЛВС;

б) прекратить обмен МНИ с зараженным СВТ;

в) лечение файловой системы серверов производить в режиме аварийного восстановления с использованием загрузочного диска производителя антивирусного ПО, с актуальными базами вирусных сигнатур;

г) после лечения СВТ последовательно подключать их к сети;

д) постоянно контролировать отсутствие вирусов на серверах;

е) замена паролей всех учетных данных, используемых на данной машине, в том числе паролей информационных систем.

10.3. После восстановления работоспособного состояния ЛВС,

СВТ, администратор антивирусной защиты производит анализ ситуации, определяет причины заражения ЛВС и виновных в нарушении, предлагает руководству ОГВ организационные и технические мероприятия по устранению в дальнейшем возможных причин заражения.

Приложение № 1 к политике

Регламент действий администратора антивирусной защиты по настройке антивирусного программного комплекса «Dr.Web Enterprise Security Suite»

1. Введение

В документе изложены обязательные действия администратора антивирусной защиты и изменения настроек компонентов антивирусной защиты (далее АВЗ) Dr.Web на узлах сети относительно настроек, сделанных производителем по умолчанию. Все настройки осуществляются через веб-интерфейс Сервера Dr.Web.

2. Основные настройки Dr.Web Enterprise Suite (вкладка «Администрирование» Сервера Dr.Web)

2.1. Администратор антивирусной защиты обязан:

2.1.1. Следить за актуальностью используемых лицензий компонентов антивирусной системы на странице «Администрирование» — «Менеджер лицензий». В случае необходимости информировать о приближении срока окончания лицензии непосредственного руководителя и участвовать в разработке и подготовке закупочной документации для приобретения лицензий и сертифицированных дистрибутивов.

2.1.2. Отслеживать результаты выполнения заданий Сервера Dr.Web (страница «Журналы» — «Журнал выполнения заданий»), настроенных на запуск по расписанию, и в случае сбоя при выполнении задачи, выявлять и устранять его причины.

2.1.3. Ежедневно контролировать актуальность вирусных сигнатур Сервера Dr.Web (страница «Репозиторий» — «Состояние репозитория») и исправлять ошибки конфигурирования параметров получения обновлений (страница «Репозиторий» — «Общая конфигурация репозитория») в случае их наличия.

2.1.4. Для оперативного отслеживания событий пользовательских компонентов АВЗ необходимо настроить отправку оповещений по электронной почте (страница «Оповещения» - «Конфигурация оповещений») на специально созданный ящик электронной почты, необходимый для получения оповещений о состоянии компонентов антивирусной защиты (пример, drweb@tularegion.ru - для администратора АВЗ ГАУ ТО «ЦИТ»). Список событий, настроенных на отправку оповещений:

а) Администратор: «Неизвестный администратор», «Ошибка авторизации администратора» (для отслеживания попыток несанкционированного получения доступа к Серверу Dr. Web),

б) Другое: «Ошибка записи журнала», «Ошибка ротации журнала», «Периодический отчет», «Соседний сервер давно не подключался», «Тестовое сообщение», «Эпидемия» (для мониторинга функционирования Сервера);

в) Новичок: «Ожидание подтверждения», «Станция отклонена автоматически», «Станция отклонена администратором» (для контроля правильности подключения новых клиентов к Серверу);

г) Ограничение лицензии: «Истек срок выдачи лицензий», «Количество

станций приближается к максимально допустимому», «Окончание срока действия агентского ключа», «Превышено допустимое количество лицензий», «Превышено допустимое количество станций» и «Превышено допустимое количество станций в базе данных» (для отслеживания соблюдения лицензионного соглашения);

д) Репозиторий: «Актуальное состояние продукта», «Мало свободного места на диске», «Обновление продукта заморожено», «Ошибка обновления продукта» и «Продукт обновлен» (для отслеживания получения обновлений сигнатур и компонентов Сервером Dr. Web);

е) Станция: «Обнаружена инфекция», «Ошибка авторизации станции», «Ошибка обновления станции», «Ошибка создания учетной записи станции», «Станция уже зарегистрирована» и «Статистика сканирования» (для отслеживания информации о функционировании клиентов);

ж) Установка: «Установка не выполнена» (уведомления об ошибках в процессе установки клиентов).

2.1.5. Необходимо настраивать выполнение заданий по расписанию (страница «Конфигурация» -> «Планировщик заданий Сервера Dr. Web»):

а) Очистка старых станций - «60». Все записи о рабочих станциях, которые 60 дней не были активны, удаляются. Некритичное;

б) Очистка старых записей - «60». Удалить все сведения на сервере администрирования старше 60 дней. Некритичное;

в) Обновление репозитория, Все продукты Dr.Web- раз в 3 часа. Критичное;

г) Резервное копирование критичных данных сервера - раз в день. Критичное.

3. Настройки антивирусной сети (вкладка «Антивирусная сеть» Сервера Dr.Web)

3.1. Все рабочие станции, подключенные к серверу администрирования, распределяются по группам администрирования (страница «Антивирусная сеть») согласно географическому или организационному принципу.

3.2. В список компонентов Dr.Web Antivirus, обязательных для установки на рабочую станцию, входят: Агент Dr.Web для Windows, Сканер Dr.Web, Агент Dr.Web для UNIX, Сканер Dr.Web для Windows, SpIDer Guard для рабочих станций Windows, SpIDer Guard для серверов Windows, SpIDer Mail для рабочих станций Windows, SpIDer Gate для рабочих станций Windows, Dr.Web Офисный контроль.

3.3. Компонент Dr.Web Firewall запрещен для установки на рабочих станциях ОГВ (для исключения конфликтов с VipNet Client, используемого для межсетевого экранирования и защиты траффика). Компоненты Dr.Web для Microsoft Outlook и Антиспам Dr.Web не устанавливаются для исключения ложных срабатываний (фильтрация нежелательной почты в ОГВ настроена на почтовых серверах).

4. Настройки Dr.Web Antivirus (рабочие станции пользователей)

4.1. Пользователю АРМ запрещено менять настройки локально установленного антивирусного ПО (Dr.Web Antivirus). Администратор АВЗ оставляет открытой для пользователя возможность создания локального расписания и переключения в мобильный режим (для ноутбуков) для своевременного получения обновлений антивирусных баз. Пользователю запрещено:

а) менять режим работы (агент всегда принимает обновления и задачи от сервера, накапливает события);

б) изменять конфигурацию Агента Dr.Web (пользователь не может настраивать уведомления, параметры подключения Агента к Серверу и синхронизации системного времени, параметры самозащиты);

в) отключение самозащиты;

г) деинсталляцию Агента Dr.Web;

д) изменять конфигурации Сканера;

е) останавливать или изменять конфигурацию Spider Guard для рабочих станций;

ё) останавливать или изменять конфигурацию Spider Guard для серверов;

ж) останавливать или изменять конфигурацию Spider Gate;

е) останавливать или изменять конфигурацию Spider Mail;

з) останавливать или изменять конфигурацию Офисного контроля Dr.Web;

и) останавливать или изменять конфигурацию превентивной защиты.

5. Список обязательных изменений настроек компонентов Dr.Web Antivirus относительно настроек по умолчанию

5.1. Действия с обнаруженными угрозами:

а) Лечить. Для инфицированных файлов;

б) Перемещение в карантин. В карантин автоматически перемещаются неизлечимые, инфицированные контейнеры, инфицированные архивы, рекламные программы, программы дозвона, программы-шутки, программы взлома. Окончательное решение по удалению или восстановлению объектов, перемещенных в карантин, принимает администратор АВЗ;

в) информирование пользователя. Осуществляется при обнаружении подозрительных или потенциально опасных программ (в том числе, программ удаленного доступа, так как у сотрудников ГАУ ТО «ЦИТ» периодически возникает производственная необходимость в их использовании для оказания технической поддержки сотрудникам ОГВ);

5.2. Исключаемые пути:

Для устранения конфликтов с модулем расчета контрольных сумм SecretNet:

- «%ProgramFiles%\Secret Net\»,
- «%ProgramFiles(x86)%\Secret Net\».

Для устранения конфликтов с ПО контроля рабочего времени:

- «c:\Windows\System32\config\systemprofile\AppData\Roaming\ TimeSvc3\»,
- «c:\Windows\System32\TimeControlSvc\»,
- «c:\Windows\System32\TimeControlSvc\Proxy\»,
- «c:\Windows\SysWOW64\TimeControlSvc\»,
- «c:\Windows\SysWOW64\TimeControlSvc\Proxy\».

5.3. Исключаемые файлы:

Для устранения конфликтов с системой DLP: IWDeployAgent.exe, iwdmc.exe, iwproxy.exe, dm.client.exe;

Для удаленной поддержки пользователей: AA_v3-5.exe;

Для устранения конфликтов с ПО VipNet Client: mftpgx.exe;

Для устранения конфликтов с ПО контроля рабочего времени: «c:\Windows\AuxiliaryService.exe»,
«c:\Windows\System32\TimeControlSvc\dpinst_64.exe»,

«c:\Windows\System32\TimeControlSvc\mediadrv32.exe»,
«c:\Windows\System32\TimeControlSvc\mediadrv64.exe»,
«c:\Windows\System32\TimeControlSvc\Proxy\LTVSrv.exe»,
«c:\Windows\System32\TimeControlSvc\Proxy\PCController.exe»,
«c:\Windows\System32\TimeControlSvc\Proxy\ProxyConfigurator.exe»,
«c:\Windows\System32\TimeControlSvc\Proxy\RegisterLSP.exe»,
«c:\Windows\System32\TimeControlSvc\Proxy\RegisterLSP64.exe»,
«c:\Windows\System32\TimeControlSvc\Proxy\
RunHiddenConsole.exe»,
«c:\Windows\System32\TimeControlSvc\sysmedia64.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\dpinst_64.exe»,
«c :\Windows\Sy s WO W64\TimeControl S vc\mediadrv3 2. exe»,
«c:\Windows\SysWOW64\TimeControlSvc\mediadrv64.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\Proxy\LTVSrv.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\Proxy\PCController.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\Proxy\
ProxyConfigurator.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\Proxy\RegisterLSP.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\Proxy\RegisterLSP64.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\Proxy\
RunHiddenConsole.exe»,
«c:\Windows\SysWOW64\TimeControlSvc\sysmedia64.exe».

5.4. Исключаемые процессы:

Для работоспособности DLP: InfoWatch.DeviceMonitor.Gui.exe, InfoWatch.DeviceMonitor.Server.exe, IWDeployAgent.exe.

5.5. Специфические настройки каждого компонента Dr.Web Antivirus:

а) Сканер. Общие настройки. «Автоматически применять действия к угрозам», «Прерывать проверку при переходе на питание от аккумулятора», «Уровень загрузки ресурсов компьютера - 25%». Действие, когда необходима перезагрузка - «Предлагать перезагрузку»;

б) SpIDer Guard для рабочих станций. Режим проверки - «Оптимальный». Не проверять файлы в локальной сети (файлы проверяются только в момент исполнения), не проверять архивы, не проверять почтовые файлы (во избежание утери архива почты за предыдущие годы);;

в) SpIDer Mail. Инфицированные сообщения - «Лечить». «Игнорировать» непроверенные, поврежденные и потенциальноопасные. Проверка почты на спам отключена (проверка осуществляется на пограничных почтовых серверах);

г) Dr.Web Офисный контроль - Доступ, включить фильтрацию WWW. Включить блокирование содержимого «Сайты о наркотиках», «Сайты о терроризме», «Сайты, связанные с азартными играми»,

«Порносайты», «Чаты», «Электронная почта», «Социальные сети» (не блокируется twitter). Не блокируется: «Сайты о насилии», «Сайты, содержащие нецензурную лексику», «Сайты об оружии».

6. Особенности настройки компонентов Dr.Web Агент на АРМ, ответственных за прием обращений граждан в ОГВ

6.1. Антивирусный монитор (SpIDer Guard G3 for Windows) Общие:

+ Использовать эвристический анализ;

+ Проверять работающие программы и модули в процессе запуска программы;

+ Оптимальный режим;

+ Блокировать автозапуск со сменных носителей;

+ Сканировать сменные устройства;

+ Перепроверять файлы после обновления вирусных баз.

6.2. SpiderMail для рабочих станций Windows

6.2.1. Общие

+ Использовать эвристический анализ.

6.2.2. Действия

+ Программы-шутки - В карантин;

+ Программы взлома - В карантин;

+ Потенциально опасные - В карантин.

Приложение № 2 к политике

Регламент действий администратора антивирусной защиты по настройки антивирусного программного комплекса «Kaspersky

Endpoint Security»

1. Введение

1.1. В документе изложены обязательные изменения настроек компонентов АВЗ Лаборатории Касперского на узлах сети, обслуживаемой ГАУ ТО «ЦИТ» относительно настроек, сделанных производителем по умолчанию.

2. Настройки Сервера администрирования

2.1. Администратор обязан настроить получение уведомлений от сервера администрирования по электронной почте о Критических событиях: «Лицензионное ограничение превышено», «Вирусная атака», «Статус компьютера «Критический», «Файл ключа в черном списке», а также об Отказах функционирования «Нет свободного места на диске» (для данных сервера администрирования или его БД), «Недоступна информационная база сервера администрирования» и «Нет свободного места в информационной базе сервера администрирования».

2.2. Также для ускорения проверки файлов и программ на вирусы необходимо согласиться с использованием облачной технологии защиты Лаборатории Касперского “KSN Proxy”. Для минимизации количества ложных предупреждений о «Вирусной атаке» необходимо увеличить кол- во обнаруженных вирусов до 20 в течение 10 минут.

2.3. Загрузку обновлений в хранилище необходимо настраивать на ежедневное выполнение, с запуском пропущенных заданий. Также в параметрах необходимо выбрать форсирование обновления подчиненных серверов.

2.4. Генерацию и рассылку отчетов сервера администрирования необходимо настроить на еженедельное выполнение на специальный сетевой ресурс, доступный руководству ГАУ ТО «ЦИТ» и комитета по инновациям и информатизации ТО для контроля состояния антивирусной защиты.

2.5. Резервное копирование данных сервера администрирования необходимо выполнять каждый день, в нерабочее время, на другой сервер и защищаться паролем. Необходимо ограничивать число хранимых резервных копий (минимум 3) во избежание нецелевого расходования свободного места на жестких дисках сервера.

3. Политика Агент администрирования Kaspersky Security Center

3.1. Активная политика. Необходимо настроить получение уведомлений по электронной почте об отказе функционирования при ошибке при установке программы агента, информационных сообщений об установке наблюдаемой программы, удалении наблюдаемой программы и установке сторонней программы.

3.2. В параметрах необходимо включить использование пароля для деинсталляции (для контроля за удалениями агента администрирования с узлов защищаемой сети).

4. Политика Kaspersky Endpoint Security for Windows

4.1. Активная политика. Необходимо настроить получение уведомлений по электронной почте о критических событиях («Базы повреждены или отсутствуют», «Базы сильно устарели», «Автозапуск программы выключен», «Обнаружен вредоносный объект») и отказе функционирования «Черный» список лицензий поврежден или не найден».

4.2. В основных параметрах настройки антивирусной защиты необходимо включать и блокировать изменения в следующих пунктах: «Запускать Kaspersky Endpoint Security для Windows при включении компьютера», включить обнаружение «Вирусы, черви, троянские программы и вредоносные утилиты»; «Рекламные программы, программы авто дозвона»; «Упакованные файлы, которые могут нанести вред, многократно упакованные файлы».

4.3. В исключения и доверенную зону компонентов антивирусной защиты необходимо добавлять папки и временные файлы почтового сервера MS Exchange, MS SQL Server и SecretNet (модуля проверки контрольных сумм).

4.4. В настройках файлового антивируса необходимо запретить пользователю его отключение. В настройках уровня безопасности «Проверка сетевых дисков» должна быть отключена для исключения замедления в работе сервера при многократной перепроверке файлов. Типы файлов для проверки - «Файлы, проверяемые по формату». Методы проверки «Эвристический анализ - поверхностный», «Проверять только новые и измененные файлы», «Проверять архивы», «Проверять установочные файлы», «Проверять вложенные OLE-объекты». Для минимизации расходования ресурсов сервера на антивирусную проверку в режиме проверки необходимо указывать «Интеллектуальный» и разрешить использование технологий «iSwift» и «iChecker».

4.5. Действие при обнаружении угрозы - «Лечить, удалять, если лечение невозможно».

4.6. Пользователю запрещено отключать почтовый антивирус. Запрещено менять уровень безопасности («рекомендуемый») и действия («Лечить, удалять, если лечение невозможно»).

4.7. Запрещено отключать веб-антивирус и менять уровень безопасности («Рекомендуемый»). Действие при обнаружении угрозы - «запрещать загрузку».

4.8. Запрещено отключать IM-Антивирус. Область защиты - входящие и исходящие сообщения. Методы проверки: проверять по базе подозрительных веб-адресов, проверять ссылки по базе фишинговых вебадресов, эвристический анализ - средний.

4.9. Мониторинг системы отключен. Компонент проактивной защиты вызывает большое количество ложных срабатываний.

4.10. В качестве средства защиты трафика в сети, обслуживаемой ГАУ ТО «ЦИТ», используются продукты линейки VipNet Custom, поэтому во избежание конфликтов компоненты «Сетевой экран» и «Защита от сетевых атак» должны быть отключены и заблокированы.

4.11. Изменения настроек защищены паролем. Необходимо, чтобы зная пароль, можно было поменять настройки на ПК, отключенном от сети.

5. Политика Антивирус Касперского для Windows Servers Enterprise Edition

5.1. Активная политика. Необходимо настроить уведомления на почтовый ящик администратора о критических событиях «Обнаружена угроза», «Базы

сильно устарели», «Срок действия лицензии истек» и отказе функционирования «Базы повреждены или некорректны».

5.2. В исключения и доверенную зону компонентов антивирусной защиты необходимо добавлять папки и временные файлы почтового сервера MS Exchange, MS SQL Server и SecretNet (модуля проверки контрольных сумм).

5.3. В параметрах хранилищ необходимо увеличить предельный размер резервного хранилища и карантина до 500 Мб. Также необходимо включить отображение значка антивирусного продукта в системном трее для быстрого локального определения статуса антивирусной защиты данного сервера.

5.4. Для обеспечения оптимального баланса производительности и глубины антивирусной проверки при выборе режимов указать «Интеллектуальный», Эвристический анализатор - «Средний», Область защиты «Жесткие диски» и «Съемные диски».

Приложение № 3 к политике

Официальные адреса электронной почты ОГВ, предназначенные для получения обращений граждан (почтовый сервер tularegion.ru).

№	Наименование ОГВ	Имя почтового ящика
1	Министерство внутренней политики и развития местного самоуправления в Тульской области	minvo@tularegion.ru
2	Министерство здравоохранения Тульской области	minzdrav@tularegion.ru
3	Министерство имущественных и земельных отношений Тульской области	mizo@tularegion.ru
4	Министерство по информатизации, связи и вопросам открытого управления Тульской области	it@tularegion.ru
5	Министерство культуры Тульской области	culture@tularegion.ru
6	Министерство молодежной политики Тульской области	gmp71 @tularegion.ru
7	Министерство образования Тульской области	do_to@tularegion.ru
8	Министерство природных ресурсов и экологии Тульской области	minecolog@tularegion.ru
9	Министерство промышленности и топливно-энергетического комплекса Тульской области	minprom@tularegion.ru
10	Министерство сельского хозяйства Тульской области	apk@tularegion.ru
11	Министерство строительства и жилищно-коммунального хозяйства Тульской области	minstrov(a),tulareeion.ru
12	Министерство транспорта и дорожного хозяйства Тульской области	mintransport@tularegion.ru
13	Министерство труда и социальной защиты Тульской области	mintrud@tularegion.ru

14	Министерство финансов Тульской области	minfin@tularegion.ru
15	Министерство экономического развития Тульской области	mineconom@tularegion.ru
16	Государственно-правовой комитет Тульской области	pravo@tularegion.ru
17	Контрольный комитет Тульской области	kontrkom@tularegion.ru
18	Комитет ветеринарии Тульской области	vetkomitet@tularegion.ru
19	Комитет Тульской области по делам записи актов гражданского состояния	komtozags@tularegion.ru
20	Комитет Тульской области по мобилизационной подготовке и связям с правоохранительными органами	mobpodg@tularegion.ru
21	Комитет Тульской области по печати и массовым коммуникациям	kompechat@tularegion.ru
22	Комитет Тульской области по предпринимательству и потребительскому рынку	smbusines@tularegion.ru
23	Комитет Тульской области по охоте и рыболовству	komoxota@tularegion.ru
24	Комитет Тульской области по развитию туризма	turizm@tularegion.ru
25	Комитет Тульской области по спорту	sport71 @tularegion.ru

26	Комитет Тульской области по тарифам	tarif@tularegion.ru
27	Государственная жилищная инспекция Тульской области	gzi71 @tularegion.ru
28	Инспекция Тульской области по государственному надзору за техническим состоянием самоходных машин и других видов техники	gtn71 @tularegion.ru
29	Инспекция Тульской области по государственной охране объектов культурного наследия	okn@tularegion.ru
30	Инспекция Тульской области по государственному архитектурностроительному надзору	igsn@tularegion.ru
31	Служба по организационному обеспечению деятельности мировых судей в Тульской области	mirsud@tularegion.ru
32	Главное управление государственной службы и кадров аппарата правительства Тульской области	glavkadry@tularegion.ru
33	Управление делами аппарата правительства Тульской области	uprdel@tularegion.ru
34	Управление пресс-службы аппарата правительства Тульской области	pressa@tularegion.ru
35	Управление протокола аппарата правительства Тульской области	protocol71 @tularegion.ru
36	Управление по делопроизводству и работе с обращениями граждан аппарата правительства Тульской области	prdelo@tularegion.ru
37	Отдел специальной документальной связи аппарата правительства Тульской области	osds@tularegion.ru

38	Отдел секретного делопроизводства аппарата правительства Тульской области	osd@tularegion.ru
39	Аппарат уполномоченных в Тульской области	apparatupolnomoc@tularegion.ru
40	Уполномоченный по защите прав предпринимателей Тульской области	ombudsmanbiz@tularegion.ru
41	Уполномоченный по правам ребенка Тульской области	tuladeti@tularegion.ru
42	Уполномоченный по правам человека Тульской области	ombutula@tularegion.ru
43	Общественная палата Тульской области	opto@tularegion.ru

Приложение № 4 к политике

Частный регламент действий администратора системы защиты пользователей корпоративной почты по настройке антивирусного программного комплекса «Kaspersky Security для Microsoft Exchange Servers»

1. Введение

1.1. В документе изложены обязательные действия администратора системы защиты пользователей корпоративной почты государственного автономного учреждения Тульской области «Центр информационных технологий» (далее - ГАУ ТО «ЦИТ») и изменения настроек компонентов системы защиты пользователей корпоративной почты (далее - СЗПКП) Лаборатории Касперского на транспортных серверах почтовой системы ГАУ ТО «ЦИТ» и обслуживаемых учреждений, в соответствии с заключенными договорами об уровне обслуживания, относительно настроек, сделанных производителем по-умолчанию. Все настройки осуществляются через интерфейс mmc-консоли продукта Kaspersky Security для Microsoft Exchange Servers каждого транспортного почтового сервера.

1.2. Программа Kaspersky Security для Microsoft Exchange Servers обязательна к установке на всех транспортных почтовых серверах ГАУ ТО «ЦИТ» и ОГВ размещенных внутри периметра сети правительства Тульской области (локальной вычислительная сеть основных зданий правительства Тульской области), для которых в соответствии с договорами об уровне обслуживания, оказывается услуга СЗПКП.

2. Основные настройки Kaspersky Security для Microsoft Exchange Servers (уровень «localhost» дерева настройки программы)

Администратор СЗПКП обязан:

2.1. Следить за актуальностью используемых лицензий программы в строке «Лицензирование». Своевременно начинать процедуры закупки, продления или расширения используемых лицензионных ключей, в соответствии с возникающими потребностями и утвержденными периодами согласования и проведения закупок. Управление ключами программы осуществляется в узле дерева настроек ПО: «localhost» -> «Лицензирование».

2.2. Отслеживать статусы основных модулей программы: «Модуль Анти-Спам: Включен», «Модуль антивирус для роли Транспортный концентратор: Включен». При необходимости устранять проблемы, повлекшие изменение статусов указанных модулей.

2.3. Контролировать (ежедневно, в срок до 10:00) актуальность баз Анти-Спама и баз Антивируса и Модуля DLP в соответствующих строках профиля настроек программы и исправлять ошибки конфигурирования параметров получения обновлений (узел дерева настроек программы «localhost» —» «Обновления») в случае их наличия.

2.4. Настроить получение уведомлений о событиях продукта Kaspersky Security для Microsoft Exchange Servers на специальный ящик электронной почты kav@tularegion.ru. Оправка уведомлений настраивается в узле дерева настроек продукта «localhost»—» «Уведомления». Список событий, которые необходимо настроить на отправку уведомлений на почтовый ящик Администратора:

а) Уведомлять о зараженных объектах (для отслеживания работы модуля «Антивирус для роли Транспортный концентратор»);

б) Уведомлять о поврежденных объектах;

в) Уведомлять о защищенных объектах (выявленные объекты, которые были защищены паролем при отправке);

г) Уведомлять о системных событиях:

- уведомлять о том, что базы устарели;
- уведомлять о событиях, связанных с лицензией;
- уведомить об истечении срока действия лицензии за: 30 дней.

д) настроить «Параметры отправки уведомлений»:

- Адрес веб-сервиса:
https://mail.tularegion.ru/ews/exchange.asmx;
Учетная запись: tularegion\kav;
- Пароль: ******* (узнать у администратора АВЗ);
- Адрес администратора: kav@tularegion.ru.

2.5. Настроить еженедельную отправку отчетов о работе программы (узел настроек «localhost» -> «Отчеты»).

Отчет по работе модуля Анти-Спам. Имя «Антиспам», тип отчета - «Анти-Спам», уровень детализации - «Стандартный», отравить - администратору. Расписание: еженедельно, Пт, 15.00.

Отчет по работе модуля Антивирус для роли Транспортный концентратор. Имя «Транспорт», тип отчета - «Антивирус для роли

Транспортный концентратор», уровень детализации - «Стандартный», отправить - администратору. Расписание: еженедельно, Пт, 15.00.

2.6. Настроить основные параметры ПО Kaspersky Security 9.0 для Microsoft Exchange Servers:

- Хранение данных: ограничить размер хранилища, размер резервного хранилища не должен превышать 76800Мб, ограничить срок хранения объектов в резервном хранилище, хранить объекты не дольше 90 дней;

- Параметры KSN. Принять положение о KSN, тем самым согласившись с использованием облачного сервиса производителя ПО для повышения точности срабатывания фильтров программы.

2.7. Настройка основных параметров работы, фильтрации входящего траффика (узел «localhost» -> «Защита сервера»).

а) Защита для роли Транспортный концентратор:

- Параметры проверки Антивируса: Зараженный объект - Удалять объект, Защищенный объект - Пропускать; Поврежденный объект - пропускать. Сохранять копию объекта в резервном хранилище;

- Параметры проверки Анти-спама. Уровень чувствительности проверки на спам: Максимальный. Результат проверки: Спам - Удалять; Возможный спам - Пропускать; Формальное оповещение - Пропускать; Внесен в черный список - Удалять; Массовая рассылка - Удалять; Фишинг Удалять;

- Параметры черного и белого списка Анти-спама. Необходимо подгрузить ранее сформированные администраторами СЗПКП списки адресатов в черный и белый списки отправителей. Добавление записей в этот список производится по необходимости, по результатам разбора писем, пересланных сотрудниками ОГВ с жалобами на нежелательную почту в адрес spam@tularegion.ru. Еженедельно подгружается новый актуализированный черный список отправителей. Белый

список актуализируется по факту получения информации от ОГВ (сотрудников).

- Белый список получателей. Фильтрация входящего траффика указанных адресов на нежелательную почту будет отключена. Подгружается список адресов, на которые необходимо обеспечить максимально возможную вероятность доставки входящих писем.